Q1. 192.168.1.102

Q2. 128.119.245.12

Sending port: 80

Receiving port: 1161

Q3. 0

The flags (0x002) tell that it is a SYN segment.

Q4. 0 and 1. Flag (0x012) tell that it is a SYNACK segment.

Q5. The sequence number is the byte number of the first byte of data in the TCP packet sent (also called a TCP segment). The acknowledgement number is the sequence number of the next byte the receiver expects to receive. So the first byte received is 1 and the next byte expected is 2026, 2025 bytes have been sent.

Q6. The sequence number is the byte number of the first byte of data in the TCP packet sent (also called a TCP segment). The acknowledgement number is the sequence number of the next byte the receiver expects to receive. So the first byte received is 1 and the next byte expected is 7866, 7865 bytes have been sent.

Q7. This makes the numbers much smaller and easier to read and compare than the real numbers which normally are initialized to randomly selected numbers in the range 0 - (2^32)-1 during the SYN phase.

Q1. It contains 4 fields, source port, destination port, length and checksum.

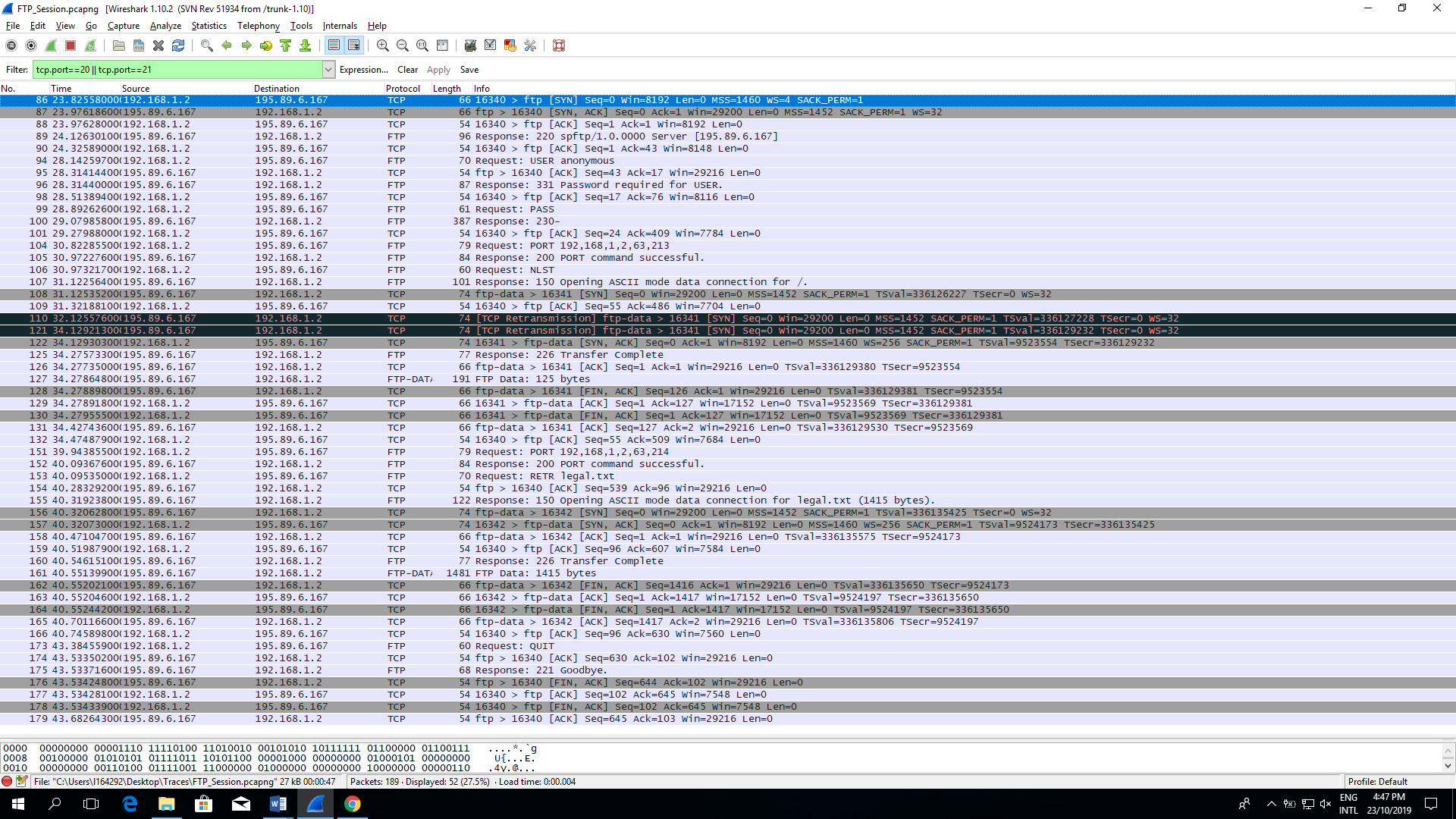
Q2. Each header is of 2 bytes.

Q3. The UDP header length field is the length of the UDP header plus the UDP data. The DNS query is of 44 bytes and the UDP header data is of 8 bytes, which equals to 52 bytes. This is equal to the length value in UDP header.

Q4. 53

|  |  |
| --- | --- |
| 1. Are ICMP messages sent over UDP or TCP? | None because it is simple request-response. |
| 1. What is the link-layer (e.g., Ethernet) address of the host? | c0:4a:00:87:05:fe |
| 1. Which kind of request is sent through these ICMP packets? | Ping request |
| 1. How many requests are sent through the host? | 4 requests |
| 1. What is the IP address of your host? What is the IP address of the destination host? | Source IP: 192.168.100.1  Dest IP: 192.168.33.110 |
| 1. Why is it that an ICMP packet does not have source and destination port numbers? | The ICMP packet was designed to communicate network-layer information between hosts and routers, not between application layer processes. |
| 1. What values in the ICMP request message differentiate this message from the ICMP reply message? | Request has type 8, reply has type 0. |
| 1. Examine one of the ping request packets sent by your host. What are the ICMP type and code numbers? What other fields does this ICMP packet have? How many bytes are the checksum, sequence number and identifier fields? | 8 and 0. Checksum, Identifier (BE) and Identifier (LE), Sequence Number (BE) and Sequence Number (LE). 2 bytes each. |
| 1. Examine the corresponding ping reply packet. What are the ICMP type and code numbers? What other fields does this ICMP packet have? How many bytes are the checksum, sequence number and identifier fields? | 0 and 0. Checksum, Identifier (BE) and Identifier (LE), Sequence Number (BE) and Sequence Number (LE). It also has data. 2 bytes each. |
| 1. Examine the packet no 56. What are the ICMP type and code numbers? Why is the IP and TCP Header included in the ICMP Header? What does these headers depict? | 3 and 3. The reason that the IP header and first 8 bytes of a datagram data in the error reporting ICMP message is included is to help you understand what conditions might have created the error message. |

Q1. After the correct FTP username and password are entered through FTP client software, the FTP server software opens port 21, which is sometimes called the command or control port, by default. Then the client makes another connection to the server over port 20 so that the actual file transfers can take place.



Q2.